International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

IJIEMR Transactions, online available on 13th Aug 2022. Link :http://www.ijiemr.org/downloads.php?vol=Volume-11&issue=Issue 08

DOI: 10.48047/IJIEMR/V11/ISSUE 08/12

Title A Novel Mechanism For Secure Data Sharing Scheme For Mobile Cloud Computing

Volume 11, ISSUE 08, Pages: 94-103

Paper Authors
A. Hemantha Kumar , S. Saikrishna

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

A Novel Mechanism For Secure Data Sharing Scheme For Mobile Cloud Computing

A. Hemantha Kumar [1], S. Saikrishna [2]

[1]Associate Professor, Dept of CSE, Audisankara College of Engineering and Technology (AUTONOMOUS), Gudur, AP, India.

[2]PG Scholar, Dept of MCA, Audisankara College of Engineering and Technology (AUTONOMOUS), Gudur, AP, India.

ABSTRACT: With the reputation of cloud computing, cell units can store/retrieve private statistics from somewhere at any time. Consequently, the statistics protection hassle in cellular cloud turns into greater and extra extreme and prevents in addition improvement of cellular cloud. There are vast research that have been carried out to enhance the cloud security. However, most of them are now not relevant for cell cloud due to the fact that cellular gadgets solely have constrained computing sources and power. Solutions with low computational overhead are in wonderful want for cellular cloud applications. In this paper, we recommend a light-weight records sharing scheme (LDSS) for cellular cloud computing. It adopts CP-ABE, an get right of entry to manipulate science used in ordinary cloud environment, however modifications the shape of get right of entry to manipulate tree to make it appropriate for cellular cloud environments. LDSS strikes a massive element of the computational intensive get entry to manipulate tree transformation in CP-ABE from cellular gadgets to exterior proxy servers. Furthermore, to minimize the person revocation cost, it introduces attribute description fields to put in force lazy-revocation, which is a thorny problem in software based totally CP-ABE systems. The experimental outcomes exhibit that LDSS can efficiently limit the overhead on the cell machine facet when customers are sharing records in cellular cloud environments.

Keywords: CP-ABE, LDSS, CLOUD SERVICE PROVIDER, ENCRYPTION, DECRYPTION, TRUSTED AUTHORITY

1. INTRODUCTION

Cloud computing ability storing information and gaining access to that statistics from the Internet as a substitute of Using Traditional hardware for most of the operations. More than 50% of IT groups have moved their Business to the cloud. Sharing of information over the cloud is the new vogue that is being set on. The quantity of statistics generated on a day to day existence is growing and to save that all of the information in regular hardware is now not feasible due to the fact of constrained storage capacity. Therefore, transferring the records to the cloud is a necessity the place the consumer can get limitless storage. Security of that information over is the subsequent huge challenge for most of us. After importing the statistics to the cloud use loses its manage over that data. Since private records archives are sensitive, facts proprietors are allowed to share information documents with statistics customers through producing a random key. Therefore, privateness of the private touchy information is a large subject for many records owners. Nowadays, a number cloud cellular purposes have been extensively used. In this applications, people(data owners) can add there archives and different archives to the cloud and share these statistics with different people(facts user) they like to share. CSPs additionally furnish statistics administration performance for facts owners. Clearly, information privateness of the private touchy statistics is massive challenge for many facts proprietors.

2.LITERATURE SURVEY

2.1 Gentry C, Halevi S. Implementing gentry's fully-homomorphic encryption scheme. in: Advances in Cryptology– EUROCRYPT 2011. Berlin, Heidelberg: Springer press, pp. 129-148, 2011.

We report a workable implementation of a variant of Gentry's completely homomorphic encryption scheme (STOC 2009), similar to the form used in Smart and Vercauteren's earlier implementation effort (PKC 2010). Smart and Vercauteren implemented the basic "somewhat homomorphic" approach, but were unable to build the bootstrapping functionality required to make the scheme work in its entirety. We demonstrate a variety of optimizations that enable us to implement the entire system, including the bootstrapping capabilities.

2.2 Brakerski Z, Vaikuntanathan V. Efficient fully homomorphic encryption from (standard) LWE. in: Proceeding of IEEE Symposium on Foundations of Computer Science. California, USA: IEEE press, pp. 97-106, Oct. 2011

We describe a fully homomorphic encryption technique that is purely based on the (traditional) learning with errors (LWE) assumption. The security of our technique is predicated on the worst-case hardness of "short vector problems" on arbitrary lattices, using established results on LWE. Our design improves on prior works in two ways: 1. Using a novel relinearization technique, we demonstrate that "somewhat homomorphic" encryption can be based on LWE. All earlier techniques, on the other hand, depended on complexity assumptions relating to ideals in various rings. 2. We depart from the "squashing paradigm" that has been adopted in all previous publications. We present a new dimension-modulus reduction strategy that shortens the ciphertexts and lowers the decryption complexity of our scheme without adding new assumptions.

2.3 Qihua Wang, Hongxia Jin. "Data leakage mitigation for discertionary access control in collaboration clouds". the 16th ACM Symposium on Access Control Models and Technologies (SACMAT), pp.103-122, Jun. 2011

With the growing popularity of cloud computing, an increasing number of businesses are converting their collaboration platforms from on-premises systems to Software as a Service (SaaS) applications. While SaaS collaboration offers many benefits, it also introduces new security problems. Because SaaS collaboration is increasingly being used across corporate boundaries, firms are afraid that sensitive information may be exposed to outsiders as a result of their employees' unintended information sharing mistakes. In this paper, we propose limiting human errors to alleviate the data leakage problem in SaaS collaboration platforms. We designed a number of procedures to enable defence in depth against information leaking on top of the discretionary access control approach in existing collaboration systems.

2.4 Adam Skillen and Mohammad Mannan. On Implementing Deniable Storage Encryption for Mobile Devices. the 20th Annual Network and Distributed System Security Symposium (NDSS), Feb. 2013

Encryption can effectively protect data secrecy. In some cases, this is insufficient because users may be compelled into providing their decryption keys. The data must be disguised in this situation so that its very existence can be denied. To solve this specific issue, steganographic techniques and defensible encryption algorithms have been developed. We investigate the feasibility and efficacy of deniable storage encryption for mobile devices in light of the recent proliferation of smartphones and tablets. We assess existing and develop new threats to plausibly deniable encryption (PDE) in a mobile setting.

2.5 Wang W, Li Z, Owens R, et al. Secure and efficient access to outsourced data. in: Proceedings of the 2009 ACM workshop on Cloud computing security. Chicago, USA: ACM pp. 55-66, 2009

Accessing vast amounts of outsourced data in a secure and effective manner is a critical component of cloud computing. We offer a technique in this work to tackle this problem in owner-write-users-read applications. We suggest encrypting each data block with a unique key in order to enable flexible cryptography-based access control. The owner just needs to keep a few secrets if key derivation methods are used. According to the analysis, the key derivation technique employing hash functions will incur relatively little compute overhead. To prevent revoked users from accessing updated data blocks, we recommend using over-encryption and/or lazy revocation. We create procedures to handle both outsourced data updates and changes in user access privileges.

2.6 Kan Yang, Xiaohua Jia, Kui Ren: Attribute-based fine-grained access control with efficient revocation in cloud storage systems. ASIACCS 2013, pp. 523-528, 2013

A cloud storage service enables data owners to outsource their data to the cloud and provide data access to consumers. The semi-trusted cloud server cannot enforce the access policy because it is not in the same trust domain as the data owner. To overcome this issue, previous techniques often entail the data owner encrypting the data and providing decryption keys to authorised users.

2.7 Crampton J, Martin K, Wild P. On key assignment for hierarchical access

control. in: Computer Security Foundations Workshop. IEEE press, pp. 14-111, 2006

A key assignment system, often known as hierarchical access control, is a cryptographic mechanism for establishing an information flow policy. To date, all research on key assignment systems has concentrated on specific encryption techniques rather than an examination of what properties are necessary in such a scheme. To address this, we present a set of generic key assignment strategies and assess their benefits.

2.8 Shi E, Bethencourt J, Chan T H H, et al. Multi-dimensional range query over encrypted data. in: Proceedings of Symposium on Security and Privacy (SP), IEEE press, 2007. 350- 364

We create a multi-dimensional range query over encrypted data (MRQED) encryption system to solve privacy problems associated with the sharing of network audit logs and other applications. Our technique enables a network gateway to encrypt network traffic summaries before submitting them to an untrusted source. When network intrusions are suspected, an authority might grant an auditor access to a key, allowing the auditor to decrypt flows whose attributes (e.g., source and destination addresses, port numbers, etc.) fall within specific ranges. However, the privacy of all irrelevant flows is maintained.

2.9 Cong Wang, Kui Ren, Shucheng Yu, and Karthik Mahendra Raje Urs. Achieving Usable and Privacy-assured Similarity Search over Outsourced Cloud Data. IEEE INFOCOM 2012, Orlando, Florida, March 25-30, 2012

As the amount of data produced by individuals and businesses that needs to be kept and used grows, data owners are tempted to outsource their local complicated data management systems to the cloud for greater flexibility and cost savings. However, because sensitive cloud data may need to be encrypted before outsourcing, rendering the typical data utilisation service based on plaintext keyword search useless, how to provide privacy-assured utilisation methods for outsourced cloud data is critical. Given the vast number of on-demand data users and the massive volume of outsourced data files in the cloud, the problem is especially problematic, since it is exceedingly difficult to meet the practical criteria of performance, system usability, and high-level user searching experiences.

2.10 Yu S., Wang C., Ren K., Lou W. Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing. INFOCOM 2010, pp. 534-542, 2010

Cloud computing is a new computing paradigm in which computing infrastructure resources are delivered as services over the Internet. As exciting as it sounds, this paradigm introduces a slew of new difficulties for data security and access control when users share sensitive data on cloud servers that are not in the same trusted domain as the data owners. Existing solutions often employ cryptographic approaches to keep sensitive user data confidential against untrusted servers by releasing data decryption keys only to authorised users.

2.11 Kan Yang, Xiaohua Jia, Kui Ren, Bo Zhang, Ruitao Xie: DACMACS: Effective Data Access Control for Multiauthority Cloud Storage Systems. IEEE Transactions on Information Forensics and Security, Vol. 8, No. 11, pp.1790-1801, 2013

Data access control is an effective way to ensure the data security in the cloud. However, due to data outsourcing and untrusted cloud servers, the data access control becomes a challenging issue in cloud storage systems. Existing access control schemes are no longer applicable to cloud storage systems, because they either produce multiple encrypted copies of the same data or require a fully trusted cloud server. Ciphertext-Policy Attribute-based Encryption (CP-ABE) is a promising technique for access control of encrypted data. It requires a trusted authority manages all the attributes and distributes keys in the system. In cloud storage systems, there are multiple authorities co-exist and each authority is able to issue attributes independently.

2.12 Stehlé D, Steinfeld R. Faster fully homomorphic encryption. in: Proceedings of 16th International Conference on the Theory and Application of Cryptology and Information Security. Singapore: Springer press, pp.377-394, 2010

In this paper, we revisit fully homomorphic encryption (FHE) based on GSW and its ring variants. We notice that the internal product of GSW can be replaced by a simpler external product between a GSW and an LWE ciphertext. We show that the bootstrapping scheme FHEW of Ducas and Micciancio (Eurocrypt 2015) can be expressed only in terms of this external product. As a result, we obtain a speed up from less than 1 second to less than 0.1 seconds. We also reduce the 1GB bootstrapping key size to 24MB, preserving the same security levels, and we improve the noise propagation overhead by replacing exact decomposition algorithms with approximate ones.

2.13 Junzuo Lai, Robert H. Deng ,Yingjiu Li ,et al. Fully secure keypolicy attribute-based encryption with constant-size ciphertexts and fast decryption. In: Proceedings of the 9th ACM symposium on Information, Computer and Communications Security (ASIACCS), pp. 239-248, Jun. 2014

Attribute-based encryption (ABE), introduced by Sahai and Waters, is a promising cryptographic primitive, which has been widely applied to implement fine-grained access control system for encrypted data. In its key-policy flavor, attribute sets are used to annotate ciphertexts and secret keys are associated with access structures that specify which ciphertexts a user is entitled to decrypt. In most existing key-policy attribute-based encryption (KP-ABE) constructions, the size of the ciphertext is proportional to the number of attributes associated with it and the decryption cost is proportional to the number of attributes used during decryption.

2.14 **Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute based encryption in: Proceedings of the 2007 IEEE Symposium on Security and Privacy (SP). Washington, USA: IEEE Computer Society, pp. 321-334, 2007.**

In many distributed systems, a user should be allowed to access data only if they have a specific set of credentials or qualities. At the moment, the only way to enforce such regulations is to use a trusted server to store the data and mediate access control. However, if any of the servers containing the data is compromised, the data's confidentiality will be jeopardised. In this research, we introduce ciphertext-policy attribute-based encryption, a system for implementing complicated access control on encrypted data. Using our techniques, encrypted data can be kept private even if the storage server is untrustworthy; additionally, our methods are resistant to collusion assaults.

3.PROPOSED SYSTEM

- We advise a Lightweight Data Sharing Scheme (LDSS) for cell cloud computing environment.
- The predominant contributions of LDSS are as follows:
- We format an algorithm referred to as LDSS-CP-ABE primarily based on Attribute-Based Encryption (ABE) approach to provide environment friendly get entry to manipulate over ciphertext.
- We use proxy servers for encryption and decryption operations. In our approach, computational intensive operations in ABE are performed on proxy servers, which considerably decrease the computational overhead on purchaser facet cellular devices. Meanwhile, in LDSS-CP-ABE, in order to keep facts privacy, a model attribute is additionally delivered to the get entry to structure. The decryption key layout is modified so that it can be despatched to the proxy servers in a impervious way.
- We introduce lazy re-encryption and description subject of attributes to minimize the revocation overhead when dealing with the person revocation problem.
- Finally, we enforce a records sharing prototype framework primarily based on LDSS.

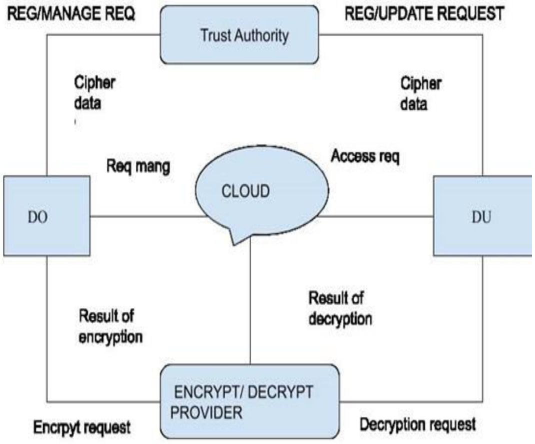


Fig : architecture diagram

The diagram contains data owner, data user, cloud, trusted authority, encryption and decryption providers.

3.1 IMPLEMENTATION

System Framework:

The improvement of cloud computing and the recognition of clever cell devices, humans are regularly getting accustomed to a new technology of records sharing mannequin in which the information is saved on the cloud and the cellular gadgets are used to store/retrieve the statistics from the cloud. In these applications, humans (data owners) can add their files and different documents to the cloud and share these records with different human beings (data users) they like to share. CSPs additionally furnish facts administration performance for information owners. Since private information documents are sensitive, records proprietors are allowed to select whether or not to make their facts archives public or can solely be shared with precise information users. Clearly, records privateness of the private touchy information is a large problem for many statistics owners. We advocate LDSS, a framework of light-weight information sharing scheme in cell cloud. It has the following six components. (1)Data Owner (DO) (2) Data User (DU) (3) Trust Authority (TA) (4) Encryption Service Provider (ESP) (5) Decryption Service Provider (DSP) (6) Cloud Service Provider (CSP).

Data Owner (DO):

When the facts proprietor (DO) registers on TA, TA runs the algorithm Setup() to generate a public key PK and a grasp key MK. PK is despatched to DO whilst MK is stored on TA itself. DO defines its very own attribute set and assigns attributes to its contacts. All these records will be despatched to TA and the cloud. TA and the cloud acquire the data and shop it. DO uploads statistics to the cell cloud and share it with friends. DO determines the get entry to manage policies. DO sends records to the cloud. Since the cloud is now not credible, statistics has to be encrypted earlier than it is uploaded. The DO defines get admission to manipulate coverage in the shape of get entry to manage tree on statistics archives to assign which attributes a DU ought to gain if he wishes to get admission to a sure records file.

Data User (DU):

When a data owner (DO) registers with TA, the algorithm Setup() is executed to generate a public key PK and a master key MK. PK is assigned to DO, but MK remains on TA. DO creates its own attribute set and assigns it to contacts. All of this data will be transferred to TA and the cloud. The information is received and stored by TA and the cloud. DO saves information to the mobile cloud and shares it with friends. DO establishes access control policies. DO transmits data to the cloud. Because the cloud is untrustworthy, data must be encrypted before being uploaded. The DO defines access control policy on data files in the form of an access control tree..

Trusted Authority:

To make LDSS viable in practice, a depended on authority (TA) is introduced. It is accountable of producing public and personal keys, and distributing attribute keys to users. With this mechanism, customers can share and get entry to records except being conscious of the encryption and decryption operations. We anticipate TA is absolutely credible, and a relied on channel exists between the TA and each user. The truth that a depended on channel exists doesn't suggest that the facts can be shared thru the depended on channel, for the facts can be in a massive amount. TA is solely used to switch keys (in a small amount) securely between users. In addition, it's requested that TA is on-line all the time due to the fact information customers might also get admission to facts at any time and want TA to replace attribute keys.

Cloud Service Provider:

DO's data is stored in CSP. It genuinely conducts the operations required by DO, and it may inspect data stored in the cloud by DO. DU makes a data request to the cloud. The cloud receives the request and determines whether the DU fits the access requirements. If DU cannot meet the condition, the request is denied; otherwise, the ciphertext is sent to DU. The Uploaded Files are managed by CSP.

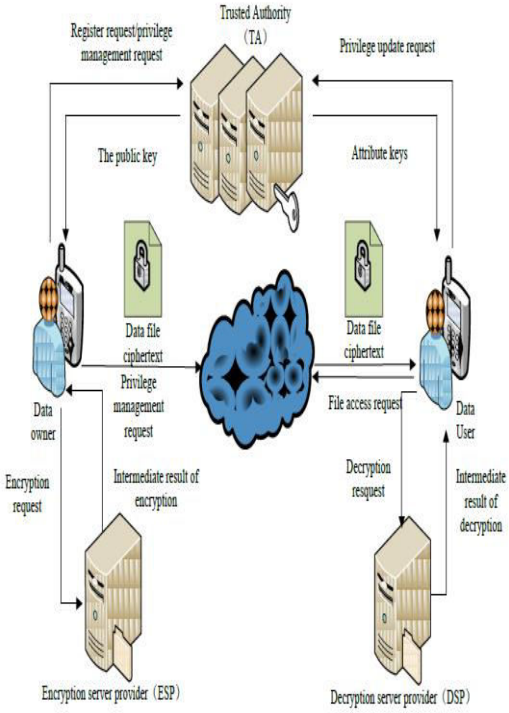
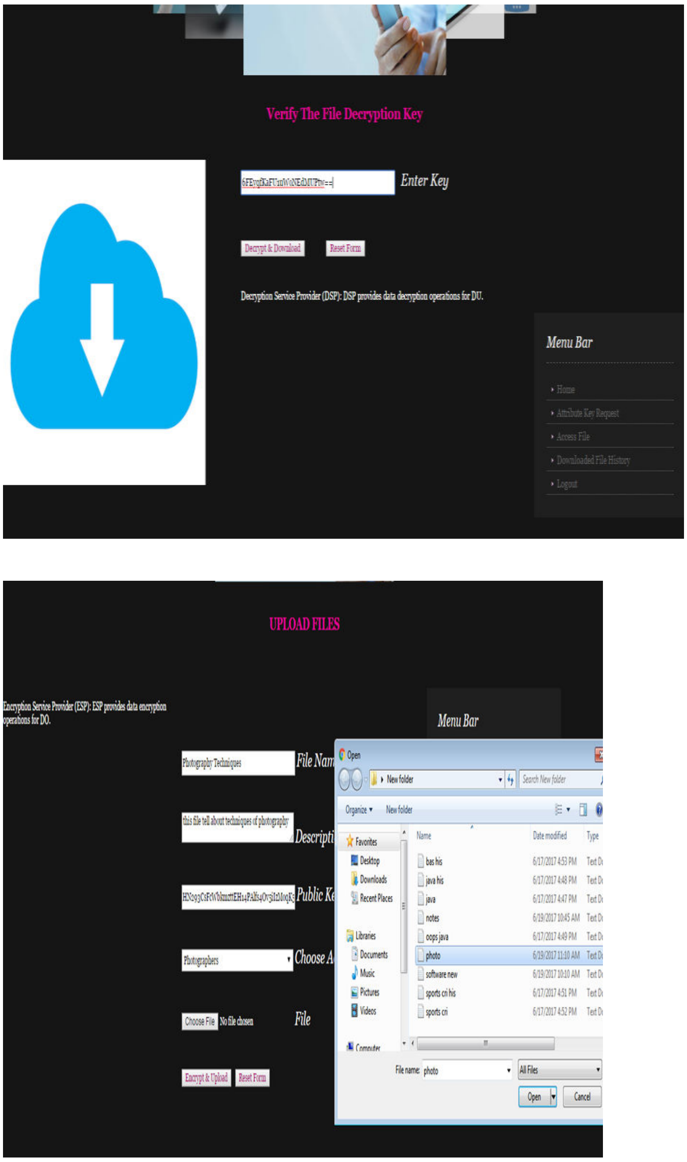

Register request/privilege management request
Trusted Authority (TA)
Privilege update request
The public key
Attribute keys
Data file ciphertext
Data file ciphertext
Privilege management request
File access request
Data owner
Data User
Encryption request
Intermediate result of encryption
Decryption resquest
Intermediate result of decryption
Encryption server provider (ESP)
Decryption server provider (DSP)

FIG 1:Architecture

4.RESULTS AND DISCUSSION


Verify The File Decryption Key

6FEvqfKaFUinWoNEdMUPtw== Enter Key

Decrypt & Download Reset Form

Decryption Service Provider (DSP): DSP provides data decryption operations for DU.

UPLOAD FILES

Encryption Service Provider (ESP): ESP provides data encryption operations for DO.

Photography Techniques File Nam

this file tell about techniques of photography Descripti

HN293CsFcWblmzttEH14PAlfs4Ov3iIzMoqK3 Public Ke

Photographers Choose A

Choose File No file chosen File

Encrypt & Upload Reset Form

Name	Date modified	Type
bas his	6/17/2017 4:53 PM	Text D
java his	6/17/2017 4:48 PM	Text D
java	6/17/2017 4:47 PM	Text D
notes	6/19/2017 10:45 AM	Text D
oops java	6/17/2017 4:49 PM	Text D
photo	6/19/2017 11:10 AM	Text D
software new	6/19/2017 10:10 AM	Text D
sports cri his	6/17/2017 4:51 PM	Text D
sports cri	6/17/2017 4:52 PM	Text D

File name: photo All Files

Open Cancel

Fig 3: Downloading data

5.CONCLUSION

In latest years, many research on get entry to manage in cloud are primarily based on attribute-based encryption algorithm (ABE). However, normal ABE isnot appropriate for cellular cloud due to the fact it is computationally intensive and cellular units solely have constrained resources. In this paper, we advocate

LDSS to tackle this issue. It introduces a novel LDSS-CP-ABE algorithm to migrate important computation overhead from cellular units onto proxy servers, consequently it can resolve the invulnerable statistics sharing hassle in cellular cloud. The experimental consequences exhibit that LDSS can make sure records privateness in cellular cloud and minimize the overhead on users' aspect in cell cloud. In the future work, we will diagram new procedures to make sure facts integrity. To in addition faucet the plausible of cellular cloud, we will additionally find out about how to do cipher textual content retrieval over current facts sharing schemes.

REFERENCES

[1] Gentry C, Halevi S. Implementing gentry's fully-homomorphic encryption scheme. in: Advances in Cryptology–EUROCRYPT 2011. Berlin, Heidelberg: Springer press, pp. 129-148, 2011.

[2] Brakerski Z, Vaikuntanathan V. Efficient fully homomorphic encryption from (standard) LWE. in: Proceeding of IEEE Symposium on Foundations of Computer Science. California, USA: IEEE press, pp. 97-106, Oct. 2011.

[3] Qihua Wang, Hongxia Jin. "Data leakage mitigation for discertionary access control in collaboration clouds". the 16th ACM Symposium on Access Control Models and Technologies (SACMAT), pp.103-122, Jun. 2011.

[4] Adam Skillen and Mohammad Mannan. On Implementing Deniable Storage Encryption for Mobile Devices. the 20th Annual Network and Distributed System Security Symposium (NDSS), Feb. 2013.

[5] Wang W, Li Z, Owens R, et al. Secure and efficient access to outsourced data. in: Proceedings of the 2009 ACM workshop on Cloud computing security. Chicago, USA: ACM pp. 55-66, 2009.

[6] Kan Yang, Xiaohua Jia, Kui Ren: Attribute-based fine-grained access control with efficient revocation in cloud storage systems. ASIACCS 2013, pp. 523-528, 2013.

[7] Crampton J, Martin K, Wild P. On key assignment for hierarchical access control. in: Computer Security Foundations Workshop. IEEE press, pp. 14-111, 2006.

[8] Shi E, Bethencourt J, Chan T H H, et al. Multi-dimensional range query over encrypted data. in: Proceedings of Symposium on Security and Privacy (SP), IEEE press, 2007. 350- 364

[9] Cong Wang, Kui Ren, Shucheng Yu, and Karthik Mahendra Raje Urs. Achieving Usable and Privacy-assured Similarity Search over Outsourced Cloud Data. IEEE INFOCOM 2012, Orlando, Florida, March 25-30, 2012

[10] Yu S., Wang C., Ren K., Lou W. Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing. INFOCOM 2010, pp. 534-542, 2010

[11] Kan Yang, Xiaohua Jia, Kui Ren, Bo Zhang, Ruitao Xie: DACMACS: Effective

Data Access Control for Multiauthority Cloud Storage Systems. IEEE Transactions on Information Forensics and Security, Vol. 8, No. 11, pp.1790-1801, 2013.

[12] Stehlé D, Steinfeld R. Faster fully homomorphic encryption. in: Proceedings of 16th International Conference on the Theory and Application of Cryptology and Information Security. Singapore: Springer press, pp.377-394, 2010.

[13] Junzuo Lai, Robert H. Deng ,Yingjiu Li ,et al. Fully secure keypolicy attribute-based encryption with constant-size ciphertexts and fast decryption. In: Proceedings of the 9th ACM symposium on Information, Computer and Communications Security (ASIACCS), pp. 239-248, Jun. 2014.

[14] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute based encryption in: Proceedings of the 2007 IEEE Symposium on Security and Privacy (SP). Washington, USA: IEEE Computer Society, pp. 321-334, 2007.

Author's Profile

A. HEMANTHA KUMAR(**hemaa.kota@gmail.com**) has received his M.Tech degree in CSE from Sathyabama Deemed University in 2006, Chennai.He is dedicated to teaching field from 2001. He has guided P.G and U.G students. His research areas included Computer Networks, Network Security and Machine Learning. At present he is working as Associate Professor in Audisankara College of Engineering and Technology, Gudur, Tirupati(Dt), Andhra Pradesh, India.

SADANALA SAIKRISHNA (**user.naidu@gmail.com**) has Pursuing his MCA from Audisankara College of Engineering and Technology (AUTONOMOUS), Gudur, affiliated to JNTUA in 2022. Andhra Pradesh, India.